

Цели и задачи

Цель лабораторной работы

Изучение задачи дискретного логарифмирования.

Выполнение лабораторной работы

Задача дискретного логарифмирования

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x , удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы.

p -алгоритм Поллрада

- Вход. Простое число p , число a порядка r по модулю p , целое число b $1 < b < p$; отображение f , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
 - Выход. показатель x , для которого $a^x = b \pmod{p}$, если такой показатель существует.
- Выбрать произвольные целые числа u, v и положить $c = a^u b^v \pmod{p}$, $d = c$
 - Выполнять $c = f(c) \pmod{p}$, $d = f(d) \pmod{p}$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r , до получения равенства $c = d \pmod{p}$
 - Приняв логарифмы для c и d , вычислить логарифм x решением сравнения по модулю r .
Результат x или РЕШЕНИЯ НЕТ.

Оценка сложности

Алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Пример работы алгоритма

```
66 def verify(g, h, p, x):  
67     return pow(g, x, p) == h  
68  
69 args = [(10, 64, 107)]  
70  
71 for arg in args:  
72     res = pollrad(*arg)  
73     print(arg, ' : ', res)  
74     print("Validates: ", verify(arg[0], arg[1], arg[2], res))
```

```
(10, 64, 107) : 20  
Validates: True
```

```
[ ] 1
```

{ #fig:001 }

Выводы

Результаты выполнения лабораторной работы

Изучили задачу дискретного логарифмирования.